



IAM Implementation : Best Practices

Danny Cheong
danny.cheong@xynapse-asia.com

The DO's
for
Identity & Access Management
Solution



Do exploit centralized IAM architecture for new and future applications

- ❖ Seek to centralized the authentication to LDAP repository
- ❖ Move towards Web Application portfolio that can be managed by a Web Access Management (WAM) solution
- ❖ Future application should be integrated directly to the WAM platform to unify the organization policies across the board
- ❖ This is feasible with Sun Directory Server and Sun Access Manager



Do use strong authentication

- ❖ Strong Identity physical identification & access and logical access solution (via ID badge and/or token/smart card) in a unify form
- ❖ Increase the security level to your organization, provide greater user convenience and reduced password-management costs



Do implement a centralized IAM audit repository

- ❖ The Forth "A" = AUDIT
- ❖ Logging of the 3A's events from IAM solution (Authentication, Authorization, Administration)
- ❖ Support respective format such as text file, CSV and XML that are easily consumable by SIEM solution
- ❖ Reduce the effort required to produce security, audit and compliance reports required on the daily, weekly or even monthly bases

Do include audit costs when justifying an IAM investment

- ❖ Consider some customization cost required for the security, audit and compliance reports from the IAM solution
- ❖ Consider to leverage on a third party reporting tools for future reporting requirements
- ❖ Sharp reductions in the time, effort and future compliance cost to produce these reports can help to justify the investment

Do create a cross-unit/cross-geography project with a senior-level commitment

- ❖ Force of significant business-process changes and rationalization across multiple business units and geographies
- ❖ Makes higher management commitment essential

Do engage a Systems Integrator for any large-scale IDM project

- ❖ IDM implementation is about business process revisions and formalization. Which is more than a technology integration
- ❖ YOU should also consider to get YOUR internal IT staff (technical staff) to involve during the development and deployment stage of a IAM implementation

The **DONT's**
for
Identity & Access Management
Solution

Don't expect to use a single authoritative source of user information

- ❖ Source of Authoritative should come from multiple source such as e-mail systems, employee contact information systems and HR related systems for employee profiles
- ❖ Expect some “decision making” difficulties and delays when it comes to SOA selection
 - Rule-of-Thumb : Get various stakeholders involve at the very beginning stage and get commitment from them

Don't aim for a single enterprise directory

- ❖ Choose to have a separated directory for internal employees and external users
- ❖ Converting applications, portals, legacy to a consolidated single directory is a painful cycle and is expensive. Let IAM solution handles it from the identity perspective
- ❖ What would be the impact, security and performance in a consolidated enterprise directory?

Don't use your enterprise authentication directory as the authoritative repository for the provisioning

- ❖ Authentication directory Vs. reporting profile and access control information
- ❖ Authentication and User Profiling performance will get affected

Don't try to integrate all applications at once

- ❖ Limit the complexity & identified achievable goals
- ❖ Start small with high-impact resources as initial target
- ❖ Begin with a friendly department
 - One that is already interested in the benefits of the IAM project and its associated application
 - Or start with enterprise infrastructure application which is widely used



Automate Your HardWork !!

Thank You